UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/796,214	03/10/2004	Toshihisa Nakano	2004-0385A	2392

52349 7590 04/04/2008

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
SCHMIDT, KARL	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
04/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/796,214	NAKANO ET AL.	
	Examiner	Art Unit	
	KARI L. SCHMIDT	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 July 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/22/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 36-42 are rejected under 35 U.S.C. 101 because claims 36-42 are directed to "computer program products" stored in a "computer readable medium". Generally, functional descriptive material, such as a computer program, is statutory when it is stored on a tangible computer readable medium. See MPEP § 2106 IV.B.I (a). However, in the present application, the specification defines "computer readable medium" to include, for example, paper or various transmission media (see at least, [0666]-[0667]). A computer program listing on a sheet of paper is not considered to provide functionality, and is therefore considered to be merely a computer program per se, which is non-statutory subject matter. Further, "transmission media" such as "communications links" as broadly defined may include non-tangible media such as signals, which are also considered non-statutory. When a claim encompasses both statutory and non-statutory subject matter, the claim as a whole is directed to non-statutory subject matter.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 15, 19, 34-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell et al. (US 6,367,019 B1) in view of Bell et al. (US 2004/0156503 A1) and Okaue (US 2002/0094088 A1).

Claims 1, 2, 19, 35, 36, 38, 39, 41, and 42

Ansell discloses a digital work protection system including a recording apparatus and a plurality of reproduction apparatuses (see at least, col. 7, line 65-col. 8, line 5 and FIG. 1: the examiner notes the recording apparatus (player 110) and the reproduction apparatus (150)), the recording apparatus being operable to encrypt content and write the encrypted content onto a recording medium (see at least, col. 5, lines 19-39 and col. 6, line 66-col. 7, lines 4 and col. 7, line 65-col. 8, line 5 and FIG. 1 and 6: the examiner notes that player 110 encrypts the content of one or more tracks and can store the encrypted content onto a recording medium (e.g. compact disc)), and the plurality of reproduction apparatuses each being operable to attempt to decrypt the encrypted content recorded on the recording medium (see at least, col. 7, lines 38-48 and FIG. 1 and 7: the examiner notes that the portable player can decrypt and playback the encrypted content), the recording medium has (i) a read-only unrewritable area in which

a medium inherent number inherent to the recording medium is prestored (see at least, col. 6, lines 8-19: the examiner notes the media identification number represents a read-only serial number) and (ii) a rewritable area to and from which data can be written and read (see at least, col. 5, lines 19-39 and col. 6, lines 54-58: the examiner notes a storage area to write data (e.g. CD-R)), and the recording apparatus includes: a storing unit that stores therein a piece of media key data including a plurality of encrypted media keys generated by (i) for each of reproduction apparatuses, encrypting a media key using a device key of the reproduction apparatus respectively (see at least, col. 7, lines 14-37: the examiner notes the master media key is encrypted with the storage key (e.g. device key) which is specific to each reproduction apparatus), a reading unit operable to read the medium inherent number from the unrewritable area of the recording medium (see at least, col. 5, line 65-col. 6, line 19: the examiner notes a serial number is specific to each respective medium and is able to be read into a binding header), an encrypting unit operable to encrypt the content being a piece of digital data, so as to generate the encrypted content (see at least, col. 6, lines 54-58: the examiner notes the use of a media master key to encrypt data), a reading unit operable to read the piece of media key data from the storing unit (see at least, col. 5, line 65-col. 6, line 7: the examiner notes the header data contains a encrypted media master key); and a writing unit operable to write the read piece of media key data and the generated encrypted content into the rewritable area of the recording medium (see at least, col. 5, line 65-col. 6, line 7: the examiner notes the binding header is on a medium and contains a encrypted media master key), and each of the reproduction apparatuses

includes: a reading unit operable to read one encrypted media key that corresponds to the reproduction apparatus, from the piece of media key data recorded in the rewritable area of the recording medium (see at least, col. 7, lines 14-48: the examiner notes the portable player can read the media master key); a decrypting unit operable to decrypt the read encrypted media key using the device key of the reproduction apparatus, so as to generate a decryption media key (see at least, col. 7, lines 14-48: the examiner notes the portable player can further decrypt the media master key); a controlling unit operable to judge whether the generated decryption media key is the detection information or not, to prohibit the encrypted content from being decrypted when having judged in the affirmative, and to permit the encrypted content to be decrypted when having judged in the negative (see at least, col. 7, lines 14-48 and col. 8, lines 19-30: the examiner notes the portable player can only decrypt and play encrypted if the binding header matches the storage key of the player if not the playback is aborted); and a decrypting unit operable to, when the encrypted content is permitted to be decrypted, read the encrypted content from the recording medium and decrypt the read encrypted content based on the generated decryption media key, so as to generate a decrypted content (see at least, col. 7, lines 14-48: the examiner notes the portable player can decrypt and play encrypted if the binding header matches the storage key of the player).

Ansell fails to disclose wherein one or more of the plurality of reproduction apparatuses are revoked; and the recording apparatus can encrypt a media key using the device key of the unrevoked reproduction apparatus and for each of the revoked

reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively; a generating unit operable to generate an encryption key based on the read medium inherent number and the media key; and an encrypting unit operable to encrypt the digital data content based on the generated encryption key in order to generate the encrypted content on the recording medium; a reading unit operable to read the piece of media key data from the storing unit; and a writing unit operable to write the read piece of media key data and the generated encrypted content into the rewritable area of the recording medium, and judging of predetermined detection information to allow content playback.

However Bell discloses a generating unit operable to generate an encryption key based on the read medium inherent number and the media key (see at least, [0043]: the examiner notes the use of the media identification and media key to create a cryptographic content key); an encrypting unit operable to encrypt the content being a piece of digital data, based on the generated encryption key, so as to generate the encrypted content (see at least, [0043]: the examiner notes the use of the cryptographic content key to encrypt the data copied to the blank disk); a reading unit operable to read the piece of media key data from the storing unit (see at least, [0043]: the examiner notes the use of the cryptographic content key to encrypt the data copied to the blank disk); and a writing unit operable to write the read piece of media key data and the generated encrypted content into the rewritable area of the recording medium (see at least, [0043]: the examiner notes the use of the cryptographic content key to encrypt the data copied to the blank disk).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell's master media key to include a generating unit operable to generate an encryption key based on the read medium inherent number and the media key; an encrypting unit operable to encrypt the content being a piece of digital data, based on the generated encryption key, so as to generate the encrypted content; a reading unit operable to read the piece of media key data from the storing unit; and a writing unit operable to write the read piece of media key data and the generated encrypted content into the rewritable area of the recording medium as taught by Bell. One of ordinary skill in the art would have been motivated to combine the teachings in order to secure the data on the disk by not allowing an unauthorized copyist to correctly calculate the media key and thus cannot correctly calculate the content key (see at least, Bell, [0044]).

Ansell in view of Bell fails to disclose wherein one or more of the plurality of reproduction apparatuses are revoked, and the recording apparatus includes can encrypt a media key using a device key of the unrevoked reproduction apparatus respectively and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively.

However Okaue discloses wherein one or more of the plurality of reproduction apparatuses are revoked (see at least, [0127]: the examiner notes that a revoked device can not acquire the content key to decode and utilize the data), and the recording apparatus includes can encrypt a media key using a device key of the unrevoked

reproduction apparatus respectively (see at least, [0125]-[0127] and [0603]-[607]: the examiner notes unrevoked devices use the node key (e.g. device key) of each respective device for encrypting data) and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively (see at least, [0125]-[0127] and [0603]-[607]: the examiner notes revoked devices are noted as revoked based on the node key of each respective device), judging of predetermined detection information to allow content playback (see at least, [0125]-[0127] and [0603]-[607]: the examiner notes that the node key is used to determine if an apparatus revoked or unrevoked).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell to include wherein one or more of the plurality of reproduction apparatuses are revoked, and the recording apparatus includes can encrypt a media key using a device key of the unrevoked reproduction apparatus respectively and (ii) for each of the revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively, judging of predetermined detection information to allow content playback as taught by Okaue. One of ordinary skill in the art would have been motivated to combine the teachings in order prevent access to secure data from devices that have had key leakage which would allow access to the secure data by unauthorized devices (see at least, Okaue, [0125]).

Claims 15 and 34

Ansell discloses wherein the first piece of media key data stored in the storing unit further includes a first data identifier that identifies the first piece of media key data (see at least, col. 5, line 65-col. 6, line 7: the examiner notes the binding header data contains data which is utilized to identify the encrypted master media key), the writing unit (i) writes the first data identifier and the encrypted content into the rewritable area of the first recording medium in such a manner that the first data identifier and the encrypted content are in correspondence with each other (see at least, col. 5, line 65-col. 6, line 7 and col. 6, lines 59-65: the examiner notes the binding header utilizes data which contains where the encrypted content is written and how its blinded together with the media key), and (ii) writes the first piece of media key data including the first data identifier into the rewritable area (see at least, col. 5, line 65-col. 6, line 7 and col. 6, lines 59-65: the examiner notes the binding header utilizes data to identify the media key which is written on the disc).

Claim 37

Ansell discloses the recording-purpose computer program of claim 36, being recorded on a computer-readable recording medium (see at least, col. 4, lines 19-34).

Claim 40

Ansell discloses the reproduction-purpose computer program of claim 39, being recorded on a computer-readable recording medium (see at least, col. 4, lines 19-34).

Claims 3-5, and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell et al. (US 6,367,019 B1) in view of Bell et al. (US 2004/0156503 A1) and Okaue (US 2002/0094088 A1) as applied to claim 2 and 15 above, and further in view of Lotspiech (US 6,609,116 B1).

Claim 3

Ansell in view of Bell and Okaue all fail to disclose wherein a second recording medium stores therein a second piece of media key data including another set of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting the media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively, and the recording apparatus further includes: a comparing unit operable to compare the second piece of media key data recorded on the second recording medium with the first piece of media key data stored in the storing unit so as to judge which is newer; and an updating unit operable to, when the second piece of media key data has been judged newer, read the second piece of media key data from the second recording medium and overwrite the first piece of media key data stored in the storing unit with the second piece of media key data, and the second reading unit reads the second piece of media key data from the storing unit, instead of the first piece

of media key data, and the writing unit writes the second piece of media key data, instead of the first piece of media key data, into the rewritable area.

However Lotspiech discloses wherein a second recording medium stores therein a second piece of media key data including another set of encrypted media keys generated (see at, least col. 3, lines 19-24: the examiner notes content disks can be recorded medium and col. 3, lines 39-46: the examiner notes updating encryption data on the medium based on new keys (e.g. player-recorder)) by (i) for each of unrevoked reproduction apparatuses, encrypting the media key using a device key of the unrevoked reproduction apparatus respectively (see at least, col. 4, line 49-col. 5, line 2: the examiner notes the use of device key's for unrevoked devices and encrypting content based of the device key's (e.g. old and new keys)) and (ii) for each of revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively (see at least, col. 5, line 57-col. 6, line 8: the examiner notes compromised keys are noted for given devices), and the recording apparatus further includes: a comparing unit operable to compare the second piece of media key data recorded on the second recording medium with the first piece of media key data stored in the storing unit so as to judge which is newer (see at least, col. 5, lines 26-34: the examiner notes the use of levels and age for seeing if a key is newer); and an updating unit operable to, when the second piece of media key data has been judged newer, read the second piece of media key data from the second recording medium and overwrite the first piece of media key data stored in the storing unit with the second piece of media key data, and the second reading unit reads the

second piece of media key data from the storing unit, instead of the first piece of media key data, and the writing unit writes the second piece of media key data, instead of the first piece of media key data, into the rewritable area (see at least, col. 6, lines 35-55: the examiner notes the use of the "newer media" key to encrypt data when it is judged whose key level is higher which written to the media (e.g. player-recorder)).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein a second recording medium stores therein a second piece of media key data including another set of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting the media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively, and the recording apparatus further includes: a comparing unit operable to compare the second piece of media key data recorded on the second recording medium with the first piece of media key data stored in the storing unit so as to judge which is newer; and an updating unit operable to, when the second piece of media key data has been judged newer, read the second piece of media key data from the second recording medium and overwrite the first piece of media key data stored in the storing unit with the second piece of media key data, and the second reading unit reads the second piece of media key data from the storing unit, instead of the first piece of media key data, and the writing unit writes the second piece of media key data, instead of the first piece of media key data, into the rewritable area as taught by

Lotspiech. One of ordinary skill in the art would have been motivated to combine the teachings to account for the presence of compromised or pirate devices and protect the data on medium by utilizing new media keys (see at least, Lotspiech, col. 1, lines 53-58).

Claims 4 and 17

Ansell in view of Bell and Okaue all fail to disclose wherein the first piece of media key data stored in the storing unit includes a first piece of version information indicating a generation of the first piece of media key data, the second piece of media key data recorded on the second recording medium includes a second piece of version information indicating a generation of the second piece of media key data, and the comparing unit judges which one of the first piece of media key data and the second piece of media key data is newer by comparing the first piece of version information with the second piece of version information.

However Lotspiech discloses wherein the first piece of media key data stored in the storing unit includes a first piece of version information indicating a generation of the first piece of media key data, the second piece of media key data recorded on the second recording medium includes a second piece of version information indicating a generation of the second piece of media key data (see at least, col. 5, lines 26-34: the examiner notes the use of levels to represent the version information of the media key), and the comparing unit judges which one of the first piece of media key data and the second piece of media key data is newer by comparing the first piece of version information with the second piece of version information (see at least, col. 6, lines 35-

46: the examiner notes the use of levels (e.g. version information) to judge if the media key is newer).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the first piece of media key data stored in the storing unit includes a first piece of version information indicating a generation of the first piece of media key data, the second piece of media key data recorded on the second recording medium includes a second piece of version information indicating a generation of the second piece of media key data, and the comparing unit judges which one of the first piece of media key data and the second piece of media key data is newer by comparing the first piece of version information with the second piece of version information as taught by Lotspiech. One of ordinary skill in the art would have been motivated to combine the teachings to account for the presence of compromised or pirate devices and protect the data on medium by utilizing new media keys (see at least, Lotspiech, col. 1, lines 53-58).

Claims 5 and 18

Ansell in view of Bell and Okaue all fail to disclose wherein the first piece of media key data stored in the storing unit includes a first piece of date and time information indicating a date and time at which the first piece of media key data has been generated, the second piece of media key data recorded on the second recording medium includes a second piece of data and time information indicating a date and time at which the second piece of media key data has been generated, and the comparing

unit judges which one of the first piece of media key data and the second piece of media key data is newer by comparing the first piece of date and time information with the second piece of date and time information.

However Lotspiech discloses wherein the first piece of media key data stored in the storing unit includes a first piece of date and time information indicating a date and time at which the first piece of media key data has been generated, the second piece of media key data recorded on the second recording medium includes a second piece of data and time information indicating a date and time at which the second piece of media key data has been generated (see at least, col. 5, lines 26-34: the examiner notes a "32" bit unit that represents the age (date and time) of a media key), and the comparing unit judges which one of the first piece of media key data and the second piece of media key data is newer by comparing the first piece of version information with the second piece of version information (see at least, col. 6, lines 35-46: the examiner notes the use of age judge if the key is newer).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the first piece of media key data stored in the storing unit includes a first piece of date and time information indicating a date and time at which the first piece of media key data has been generated, the second piece of media key data recorded on the second recording medium includes a second piece of data and time information indicating a date and time at which the second piece of media key data has been generated, and the comparing unit judges which one of the first piece of media key data and the second piece of

media key data is newer by comparing the first piece of date and time information with the second piece of date and time information as taught by Lotspiech. One of ordinary skill in the art would have been motivated to combine the teachings to account for the presence of compromised or pirate devices and protect the data on medium by utilizing new media keys (see at least, Lotspiech, col. 1, lines 53-58).

Claim 16

Ansell discloses the recording apparatus includes an assigning unit operable to assign the first data identifier, which is different from the second data identifier, to the first piece of media key data stored in the storing unit (see at least, 5, line 65-col. 8, line 7: the examiner notes the use of different data identifiers within a binding header).

Ansell in view of Bell and Okaue fails to disclose wherein the first recording medium further stores therein a second piece of media key data including another set of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively, the second piece of media key data includes a second data identifier that identifies the second piece of media key data.

However Lotspiech discloses wherein the first recording medium further stores therein a second piece of media key data including another set of encrypted media keys generated (see at least, col. 6, lines 22-58: the examiner notes the use of an old key

block and a new media key block which still use the old key or new key data) by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively (see at least, col. 6, lines 22-58: the examiner notes the use of a old key or new key for the encrypting of data), and (ii) for each of revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively, the second piece of media key data includes a second data identifier that identifies the second piece of media key data (see at least, col. 5, line 57-col. 6, line 8: the examiner notes that compromised players or pirated devices can exist and col. 6, lines 22-58: the use of new media key blocks for such players that have been compromised).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the first recording medium further stores therein a second piece of media key data including another set of encrypted media keys generated by (i) for each of unrevoked reproduction apparatuses, encrypting a media key using a device key of the unrevoked reproduction apparatus respectively, and (ii) for each of revoked reproduction apparatuses, encrypting predetermined detection information using a device key of the revoked reproduction apparatus respectively, the second piece of media key data includes a second data identifier that identifies the second piece of media key data as taught by Lotspiech. One of ordinary skill in the art would have been motivated to combine the teachings to account for the presence of compromised or pirate devices and protect the data on medium by utilizing new media keys (see at least, Lotspiech, col. 1, lines 53-58).

Claims 6-13, 20-25, and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell et al. (US 6,367,019 B1) in view of Bell et al. (US 2004/0156503 A1) and Okaue (US 2002/0094088 A1) as applied to claim 2 and 19 above, and further in view of Linnartz et al. (US 7,260,219 B2).

Claims 6 and 11

Ansell in view of Bell and Okaue all fail to disclose wherein the storing unit further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked, the recording apparatus further includes a signature generating unit operable to use a digital signature function on the piece of revocation data, so as to generate a piece of verification information, and the writing unit further writes the generated piece of verification information into the rewritable area of the first recording medium.

However Linnartz discloses wherein the storing unit further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked (see at least, col. 1, lines 40-44 and 6, lines 37-43: the examiner notes key specific to the recording or reproduction apparatus are noted as revoked with the data), the recording apparatus further includes a signature generating unit operable to use a digital signature function on the piece of revocation data, so as to generate a piece of verification information, and the writing unit further writes the generated piece of verification information into the rewritable area of the first recording medium (see at least, ,col. 4, lines 26-32: the

examiner notes a list of indicated the revoked apparatuses within data on the medium and col. 4, lines 54-64: the examiner notes that a digital signature is stored within the data on the medium as a verification of the apparatus). The examiner further notes the revoked list and data can be reproduced on a second medium.

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the storing unit further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked, the recording apparatus further includes a signature generating unit operable to use a digital signature function on the piece of revocation data, so as to generate a piece of verification information, and the writing unit further writes the generated piece of verification information into the rewritable area of the first recording medium as taught by Linnartz.. One of ordinary skill in the art would have been motivated to combine the teachings in order to store/play data in a tamper-resistant manner for a corresponding recoding apparatus and playback apparatus (see at least, Linnartz, col. 2, lines 11-16).

Claims 7 and 21

Ansell in view of Bell and Okaue all fail to disclose wherein the signature generating unit uses a digital signature with appendix on the piece of revocation data to generate a piece of signature data, so as to generate the piece of verification information from the generated piece of signature data and the piece of revocation data, and the writing unit writes the piece of verification information.

However Linnartz discloses wherein the signature generating unit uses a digital signature with appendix on the piece of revocation data to generate a piece of signature data, so as to generate the piece of verification information from the generated piece of signature data and the piece of revocation data, and the writing unit writes the piece of verification information (see at least, col. 4, lines 26-32: the examiner notes a list of indicated the revoked apparatuses within data on the medium and col. 4, lines 54-64: the examiner notes the signature is appended to the data stored in the playback section of a medium).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the signature generating unit uses a digital signature with appendix on the piece of revocation data to generate a piece of signature data, so as to generate the piece of verification information from the generated piece of signature data and the piece of revocation data, and the writing unit writes the piece of verification information as taught by Linnartz.. One of ordinary skill in the art would have been motivated to combine the teachings in order to store/play data in a tamper-resistant manner for a corresponding recoding apparatus and playback apparatus (see at least, Linnartz, col. 2, lines 11-16).

Claims 8 and 22

Ansell in view of Bell and Okaue all fail to disclose wherein the signature generating unit uses a digital signature with message recovery on the piece of revocation data to generate the piece of verification information.

However Linnartz discloses wherein the signature generating unit uses a digital signature with message recovery on the piece of revocation data to generate the piece of verification information (see at least, col. 4, lines 26-32: the examiner notes a list of indicated the revoked recorders within the data on the medium and col. 4, lines 54-64: the examiner notes the signature is used with data stored in the playback section based on a secret private key (e.g. message recovery)).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the signature generating unit uses a digital signature with message recovery on the piece of revocation data to generate the piece of verification information as taught by Linnartz.. One of ordinary skill in the art would have been motivated to combine the teachings in order to store/play data in a tamper-resistant manner for a corresponding recoding apparatus and playback apparatus (see at least, Linnartz, col. 2, lines 11-16).

Claim 9

Ansell in view of Bell and Okaue all fail to disclose wherein the storing unit further stores therein a secret key and a public key certificate of the recording apparatus, the signature generating unit uses the digital signature function using the stored secret key, the second reading unit further reads the public key certificate from the storing unit, and the writing unit writes the read public key certificate into the rewritable area of the first recording medium.

However Linnartz discloses wherein the storing unit further stores therein a secret key and a public key certificate of the recording apparatus, the signature generating unit uses the digital signature function using the stored secret key, the second reading unit further reads the public key certificate from the storing unit, and the writing unit writes the read public key certificate into the rewritable area of the first recording medium (see at least, col. 4, lines 54-65: the examiner notes a secrete private key is used to generate a signature and a public key which are stored within data on the medium).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the storing unit further stores therein a secret key and a public key certificate of the recording apparatus, the signature generating unit uses the digital signature function using the stored secret key, the second reading unit further reads the public key certificate from the storing unit, and the writing unit writes the read public key certificate into the rewritable area of the first recording medium as taught by Linnartz.. One of ordinary skill in the art would have been motivated to combine the teachings in order to store/play data in a tamper-resistant manner for a corresponding recoding apparatus and playback apparatus (see at least, Linnartz, col. 2, lines 11-16).

Claims 10 and 13

Ansell in view of Bell and Okaue all fail to disclose wherein the storing unit further stores therein a public key certificate of the recording apparatus, the second reading unit reads the public key certificate from the storing unit, and the writing unit writes the read public key certificate into the rewritable area of the first recording medium.

However Linnartz discloses wherein the storing unit further stores therein a public key certificate of the recording apparatus, the second reading unit reads the public key certificate from the storing unit, and the writing unit writes the read public key certificate into the rewritable area of the first recording medium (see at least, col. 4, lines 54-65: the examiner notes writing a public key certificate within the storage area of the medium). The examiner further notes this could be reproduced on a second medium.

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the storing unit further stores therein a public key certificate of the recording apparatus, the second reading unit reads the public key certificate from the storing unit, and the writing unit writes the read public key certificate into the rewritable area of the first recording medium as taught by Linnartz.. One of ordinary skill in the art would have been motivated to combine the teachings in order to store/play data in a tamper-resistant manner for a corresponding recoding apparatus and playback apparatus (see at least, Linnartz, col. 2, lines 11-16).

Claim 12

Ansell in view of Bell and Okaue all fail to disclose wherein the storing unit further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked, the second reading unit further reads the piece of revocation data from the storing unit, and the writing unit writes the read piece of revocation data onto the second recording medium.

However Linnartz discloses wherein the storing unit further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked, the second reading unit further reads the piece of revocation data from the storing unit, and the writing unit writes the read piece of revocation data onto the second recording medium (see at least, col. 4, lines 24-28: the examiner notes the list of revoked devices are written in the data area of a medium and col. col. 1, lines 40-44 and 6, lines 37-43: the examiner notes key specific to the recording or reproduction apparatus are noted as revoked within the data)

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the storing unit further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked, the second reading unit further reads the piece of revocation data from the storing unit, and the writing unit writes the read piece of revocation data onto the second recording

medium as taught by Linnartz.. One of ordinary skill in the art would have been motivated to combine the teachings in order to store/play data in a tamper-resistant manner for a corresponding recoding apparatus and playback apparatus (see at least, Linnartz, col. 2, lines 11-16).

Claim 20

Ansell in view of Bell and Okaue all fail to disclose wherein the recording apparatus further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked, uses a digital signature function on the piece of revocation data to generate a piece of verification information, and writes the generated piece of verification information into the rewritable area of the first recording medium, the reading unit further reads the piece of verification information recorded in the rewritable area, the reproduction apparatus further includes a verifying unit operable to implement signature verification based on the read piece of verification information and output a verification result indicating either a verification successor a verification failure, and the controlling unit further prohibits the encrypted content from being decrypted when the verification result indicates a verification failure, and permits the encrypted content to be decrypted when the verification result indicates a verification success.

However Linnartz discloses wherein the recording apparatus further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked (col. 1,

lines 40-44 and 6, lines 37-43: the examiner notes key specific to the recording or reproduction apparatus are noted as revoked within the data) , uses a digital signature function on the piece of revocation data to generate a piece of verification information, and writes the generated piece of verification information into the rewritable area of the first recording medium, the reading unit further reads the piece of verification information recorded in the rewritable area (see at least, ,col. 4, lines 26-32: the examiner notes a list of indicated the revoked apparatuses within data on the medium and col. 4, lines 54-64: the examiner notes that a digital signature is stored within the data on the medium as a verification of the apparatus), the reproduction apparatus further includes a verifying unit operable to implement signature verification based on the read piece of verification information and output a verification result indicating either a verification successor a verification failure, and the controlling unit further prohibits the encrypted content from being decrypted when the verification result indicates a verification failure, and permits the encrypted content to be decrypted when the verification result indicates a verification success (see at least, col. 3, lines 53-65: the examiner notes the use of a cry graphic summary on the public key and signature to verify if the encrypted data can be played or not) .

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the recording apparatus further stores therein a piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked, uses a digital signature function on the piece of revocation

data to generate a piece of verification information, and writes the generated piece of verification information into the rewritable area of the first recording medium, the reading unit further reads the piece of verification information recorded in the rewritable area, the reproduction apparatus further includes a verifying unit operable to implement signature verification based on the read piece of verification information and output a verification result indicating either a verification successor a verification failure, and the controlling unit further prohibits the encrypted content from being decrypted when the verification result indicates a verification failure, and permits the encrypted content to be decrypted when the verification result indicates a verification success as taught by Linnartz.. One of ordinary skill in the art would have been motivated to combine the teachings in order to store/play data in a tamper-resistant manner for a corresponding recoding apparatus and playback apparatus (see at least, Linnartz, col. 2, lines 11-16).

Claim 23

Ansell in view of Bell and Okaue all fail to disclose wherein the recording apparatus further stores therein a secret key and a public key certificate of the recording apparatus, the recording apparatus (i) uses the digital signature function using the stored secret key, (ii) reads the public key certificate, and (iii) writes the read public key certificate into the rewritable area of the first recording medium, and the verifying unit reads the public key certificate from the first recording medium, extracts a public key from the read public key certificate, and implements the signature verification using the extracted public key.

However Linnartz discloses wherein the recording apparatus further stores therein a secret key and a public key certificate of the recording apparatus (see at least, col. 4, lines 54-64: the examiner notes a private secrete key and a public key certificate), the recording apparatus (i) uses the digital signature function using the stored secret key (see at least, col. 39-64: the examiner notes the use of a secrete private key to implement a signature), (ii) reads the public key certificate (see at least, col. 4, lines 54-64), and (iii) writes the read public key certificate into the rewritable area of the first recording medium, and the verifying unit reads the public key certificate from the first recording medium, extracts a public key from the read public key certificate, and implements the signature verification using the extracted public key (see at least, col. 4, lines 54-64: the examiner notes the public key certificate is written on the data area of a medium and col. 3, lines 53-65: the examiner notes the use of a cryptographic summary to verify the public key).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include e wherein the recording apparatus further stores therein a secret key and a public key certificate of the recording apparatus, the recording apparatus (i) uses the digital signature function using the stored secret key, (ii) reads the public key certificate, and (iii) writes the read public key certificate into the rewritable area of the first recording medium, and the verifying unit reads the public key certificate from the first recording medium, extracts a public key from the read public key certificate, and implements the signature verification using the extracted public key as taught by Linnartz.. One of ordinary skill in the art would have

been motivated to combine the teachings in order to store/play data in a tamper-resistant manner for a corresponding recoding apparatus and playback apparatus (see at least, Linnartz, col. 2, lines 11-16).

Claim 24

Ansell in view of Bell and Okaue all fail to disclose wherein the recording apparatus stores therein the piece of revocation data, uses a digital signature function on the piece of revocation data to further generate another piece of verification information, and writes the generated piece of verification information onto a second recording medium, the reading unit reads the other piece of verification information from the second recording medium instead of from the first recording medium, and the verifying unit implements the signature verification based on the other piece of verification information read from the second recording medium.

However Linnartz discloses wherein the recording apparatus stores therein the piece of revocation data, uses a digital signature function on the piece of revocation data to further generate another piece of verification information (see at least, col. 1, lines 40-44 and 6, lines 37-43: the examiner notes key specific to the recording or reproduction apparatus are noted as revoked within the data and col. 4, lines 54-65: the examiner notes a secrete private key is used to generate a signature), and writes the generated piece of verification information onto a second recording medium (col. 4, lines 54-65: the examiner notes a secrete private key is used to generate a signature), the reading unit reads the other piece of verification information from the second

recording medium instead of from the first recording medium, and the verifying unit implements the signature verification based on the other piece of verification information read from the second recording medium (col. 3, lines 53-65: the examiner notes the use of a cryptographic summary to verify the signature).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the recording apparatus stores therein the piece of revocation data, uses a digital signature function on the piece of revocation data to further generate another piece of verification information, and writes the generated piece of verification information onto a second recording medium, the reading unit reads the other piece of verification information from the second recording medium instead of from the first recording medium, and the verifying unit implements the signature verification based on the other piece of verification information read from the second recording medium as taught by Linnartz.. One of ordinary skill in the art would have been motivated to combine the teachings in order to store/play data in a tamper-resistant manner for a corresponding recoding apparatus and playback apparatus (see at least, Linnartz, col. 2, lines 11-16).

Claims 25, 31, and 32

Ansell in view of Bell and Okaue all fail to disclose wherein the recording apparatus further stores therein a public key certificate of the recording apparatus, reads the public key certificate, and writes the read public key certificate into the rewritable area of the first recording medium, the reproduction apparatus further includes: a storing unit that

stores therein a first piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked; a certificate reading unit operable to read the public key certificate from the first recording medium; and a public key verifying unit operable to check whether a public key included in the read public key certificate is revoked according to the first piece of verification data, and the controlling unit further prohibits the encrypted content from being decrypted when the public key is revoked, and permits the encrypted content to be decrypted when the public key is not revoked.

However Linnartz discloses wherein the recording apparatus further stores therein a public key certificate of the recording apparatus, reads the public key certificate, and writes the read public key certificate into the rewritable area of the first recording medium (see at least, col. 4, lines 54-64: the examiner notes the public key certificate is written on the data area of a medium), the reproduction apparatus further includes: a storing unit that stores therein a first piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked (col. col. 1, lines 40-44 and 6, lines 37-43: the examiner notes key specific to the recording or reproduction apparatus are noted as revoked within the data); a certificate reading unit operable to read the public key certificate from the first recording medium (col. 3, lines 53-65: the examiner notes the use of a cryptographic summary to verify the public key); and a public key verifying unit operable to check whether a public key included in the read public key certificate is revoked according to the first piece of verification data, and the controlling unit further

prohibits the encrypted content from being decrypted when the public key is revoked, and permits the encrypted content to be decrypted when the public key is not revoked (col. 3, lines 53-65: the examiner notes the use of a cryptographic summary to verify the public key and allow for content playback if not revoked). The examiner notes multiple revoked keys are stored within the data area of the medium and are used for verification purposes of cryptographic hashes in order to allow the content to be played.

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the recording apparatus further stores therein a public key certificate of the recording apparatus, reads the public key certificate, and writes the read public key certificate into the rewritable area of the first recording medium, the reproduction apparatus further includes: a storing unit that stores therein a first piece of revocation data indicating one or more of public keys assigned to the recording apparatus and the plurality of reproduction apparatuses are revoked; a certificate reading unit operable to read the public key certificate from the first recording medium; and a public key verifying unit operable to check whether a public key included in the read public key certificate is revoked according to the first piece of verification data, and the controlling unit further prohibits the encrypted content from being decrypted when the public key is revoked, and permits the encrypted content to be decrypted when the public key is not revoked as taught by Linnartz.. One of ordinary skill in the art would have been motivated to combine the teachings in order to store/play data in a tamper-resistant manner for a

corresponding recoding apparatus and playback apparatus (see at least, Linnartz, col. 2, lines 11-16).

Claims 26-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell et al. (US 6,367,019 B1) in view of Bell et al. (US 2004/0156503 A1) and Okaue (US 2002/0094088 A1) and Linnartz et al. (US 7,260,219 B2) as applied to claim 25 above, and further in view of Lotspiech (US 6,609,116 B1).

Claim 26

Ansell in view of Bell and Okaue and Linnartz all fail to disclose wherein the reproduction apparatus further includes: a comparing unit operable to compare the second piece of revocation data recorded on the second recording medium with the first piece of revocation data stored in the storing unit so as to judge which is newer; and an updating unit operable to, when the second piece of revocation data has been judged newer, read the second piece of revocation data from the second recording medium and overwrite the first piece of revocation data in the storing unit with the read second piece of revocation data.

Lotspiech discloses wherein the reproduction apparatus further includes: a comparing unit operable to compare the second piece of revocation data recorded on the second recording medium with the first piece of revocation data stored in the storing unit so as to judge which is newer (see at least, col. 5, lines 26-34: the examiner notes the use of levels and age for seeing if a key is newer); and an updating unit operable

to, when the second piece of revocation data has been judged newer, read the second piece of revocation data from the second recording medium and overwrite the first piece of revocation data in the storing unit with the read second piece of revocation data (see at least, col. 6, lines 35-55: the examiner notes the use of the "newer media" key to encrypt data when it is judged whose key level is higher which written to the media (e.g. player-recorder)).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue and Linnartz to include wherein the reproduction apparatus further includes: a comparing unit operable to compare the second piece of revocation data recorded on the second recording medium with the first piece of revocation data stored in the storing unit so as to judge which is newer; and an updating unit operable to, when the second piece of revocation data has been judged newer, read the second piece of revocation data from the second recording medium and overwrite the first piece of revocation data in the storing unit with the read second piece of revocation data as taught by Lotspiech. One of ordinary skill in the art would have been motivated to combine the teachings to account for the presence of compromised or pirate devices and protect the data on medium by utilizing new media keys (see at least, Lotspiech, col. 1, lines 53-58).

Claim 27

Ansell in view of Bell and Okaue and Linnartz all fail to disclose wherein the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing sizes of the first and second pieces of revocation data.

Lotspiech discloses wherein the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing sizes of the first and second pieces of revocation data (see at least, col. 6, lines 35-55: the examiner notes the use of the "newer media" key to encrypt data when it is judged whose key level (e.g. size of number 1, 2, etc) is higher which written to the media (e.g. player-recorder)).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue and Linnartz to include wherein the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing sizes of the first and second pieces of revocation data as taught by Lotspiech. One of ordinary skill in the art would have been motivated to combine the teachings to account for the presence of compromised or pirate devices and protect the data on medium by utilizing new media keys (see at least, Lotspiech, col. 1, lines 53-58).

Claim 28

Ansell in view of Bell and Okaue and Linnartz all fail to disclose wherein the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing numbers of the revoked public keys indicated by the first and second pieces of revocation data.

Lotspiech discloses wherein the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing numbers of the revoked public keys indicated by the first and second pieces of revocation data (see at least, col. 6, lines 35-55: the examiner notes the use of the CMKC (e.g. calculate media command) to judge newer keys from older keys).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue and Linnartz to include wherein the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing numbers of the revoked public keys indicated by the first and second pieces of revocation data as taught by Lotspiech. One of ordinary skill in the art would have been motivated to combine the teachings to account for the presence of compromised or pirate devices and protect the data on medium by utilizing new media keys (see at least, Lotspiech, col. 1, lines 53-58).

Claim 29

Ansell in view of Bell and Okaue and Linnartz all fail to disclose wherein the first piece of revocation data stored in the storing unit includes a first piece of version information indicating a generation of the first piece of revocation data, the second piece of

revocation data recorded on the second recording medium includes a second piece of version information indicating a generating of the second piece of revocation data, and the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing the first and second pieces of version information.

Lotspiech discloses wherein the first piece of revocation data stored in the storing unit includes a first piece of version information indicating a generation of the first piece of revocation data, the second piece of revocation data recorded on the second recording medium includes a second piece of version information indicating a generating of the second piece of revocation data, and the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing the first and second pieces of version information (see at least, col. 6, lines 35-55: the examiner notes the use of the "newer media" key to encrypt data when it is judged whose key level (e.g. version number 1, 2, etc) is higher which written to the media (e.g. player-recorder))).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue and Linnartz to include wherein the first piece of revocation data stored in the storing unit includes a first piece of version information indicating a generation of the first piece of revocation data, the second piece of revocation data recorded on the second recording medium includes a second piece of version information indicating a generating of the second piece of revocation data, and the comparing unit judges which one of the first piece of revocation data and the

second piece of revocation data is newer by comparing the first and second pieces of version information as taught by Lotspiech. One of ordinary skill in the art would have been motivated to combine the teachings to account for the presence of compromised or pirate devices and protect the data on medium by utilizing new media keys (see at least, Lotspiech, col. 1, lines 53-58).

Claim 30

Ansell in view of Bell and Okaue and Linnartz all fail to disclose wherein the first piece of revocation data stored in the storing unit includes a first piece of date and time information indicating a date and time at which the first piece of revocation data has been generated, the second piece of revocation data recorded on the second recording medium includes a second piece of date and time information indicating a date and time at which the second piece of revocation data has been generated, and the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing the first and second pieces of date and time information.

Lotspiech discloses wherein the first piece of revocation data stored in the storing unit includes a first piece of date and time information indicating a date and time at which the first piece of revocation data has been generated, the second piece of revocation data recorded on the second recording medium includes a second piece of date and time information indicating a date and time at which the second piece of revocation data has been generated, and the comparing unit judges which one of the

first piece of revocation data and the second piece of revocation data is newer by comparing the first and second pieces of date and time information (see at least, col. 5, lines 26-34: the examiner notes a "32" bit unit that represents the age (date and time) of a media key and col. 6, lines 35-55: the examiner notes the use of the "newer media" key to encrypt data when it is judged whose key age is higher which written to the media (e.g. player-recorder))).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue and Linnartz to include wherein the first piece of revocation data stored in the storing unit includes a first piece of date and time information indicating a date and time at which the first piece of revocation data has been generated, the second piece of revocation data recorded on the second recording medium includes a second piece of date and time information indicating a date and time at which the second piece of revocation data has been generated, and the comparing unit judges which one of the first piece of revocation data and the second piece of revocation data is newer by comparing the first and second pieces of date and time information as taught by Lotspiech. One of ordinary skill in the art would have been motivated to combine the teachings to account for the presence of compromised or pirate devices and protect the data on medium by utilizing new media keys (see at least, Lotspiech, col. 1, lines 53-58).

Claims 14 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell et al. (US 6,367,019 B1) in view of Bell et al. (US 2004/0156503 A1) and Okaue (US 2002/0094088 A1) as applied to claim 2 and 19 above, and further in view of Hollar (US 2002/0126842 A1).

Claims 14 and 33

Ansell in view of Bell and Okaue all fail to disclose wherein the storing unit further stores therein an apparatus identifier that identifies the recording apparatus, the recording apparatus further includes an embedding unit operable to read the apparatus identifier and embed the read apparatus identifier into the content as an electronic watermark, and the encrypting unit encrypts the content into which the apparatus identifier is embedded.

However, Hollar discloses wherein the storing unit further stores therein an apparatus identifier that identifies the recording apparatus, the recording apparatus further includes an embedding unit operable to read the apparatus identifier and embed the read apparatus identifier into the content as an electronic watermark, and the encrypting unit encrypts the content into which the apparatus identifier is embedded (see at least, abstract and [0003]-[0005]: the examiner notes the watermark is emended within the data and is used for copy protection).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Ansell in view of Bell and Okaue to include wherein the storing unit further stores therein an apparatus identifier that identifies the recording apparatus, the

recording apparatus further includes an embedding unit operable to read the apparatus identifier and embed the read apparatus identifier into the content as an electronic watermark, and the encrypting unit encrypts the content into which the apparatus identifier is embedded as taught by Hollar. One of ordinary skill in the art would have been motivated to combine the teachings protect proprietary material with the used of enhanced copy and play protection with the use of employing watermarks (see at least, Hollar, [0003]-[0005]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KARI L. SCHMIDT whose telephone number is (571)270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kari L Schmidt/
Examiner, Art Unit 2139

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139